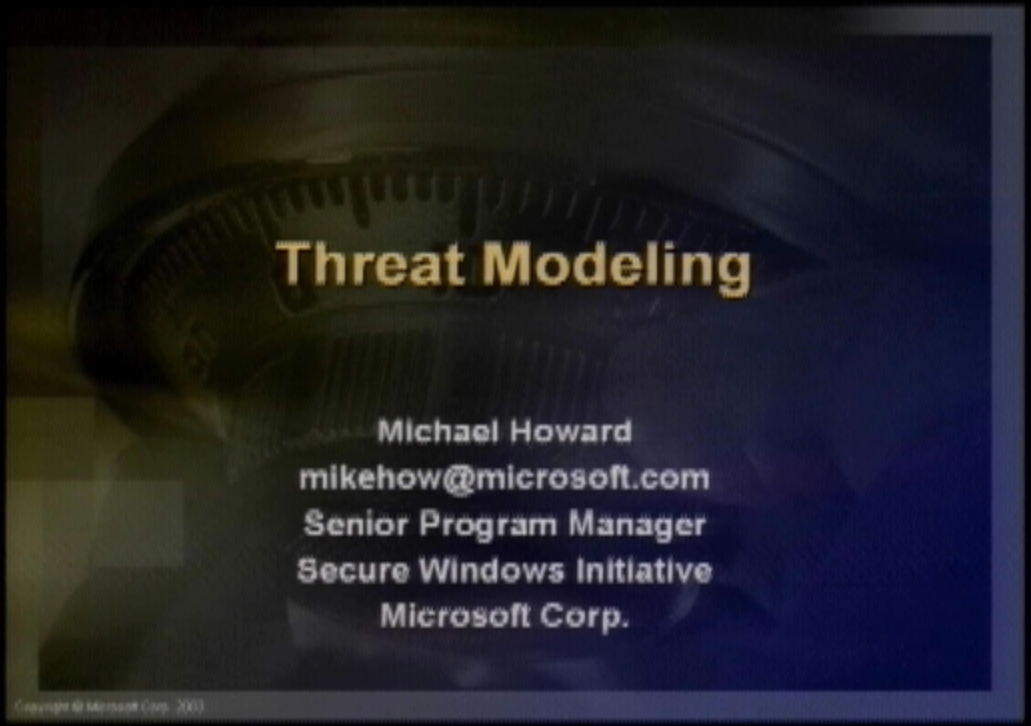
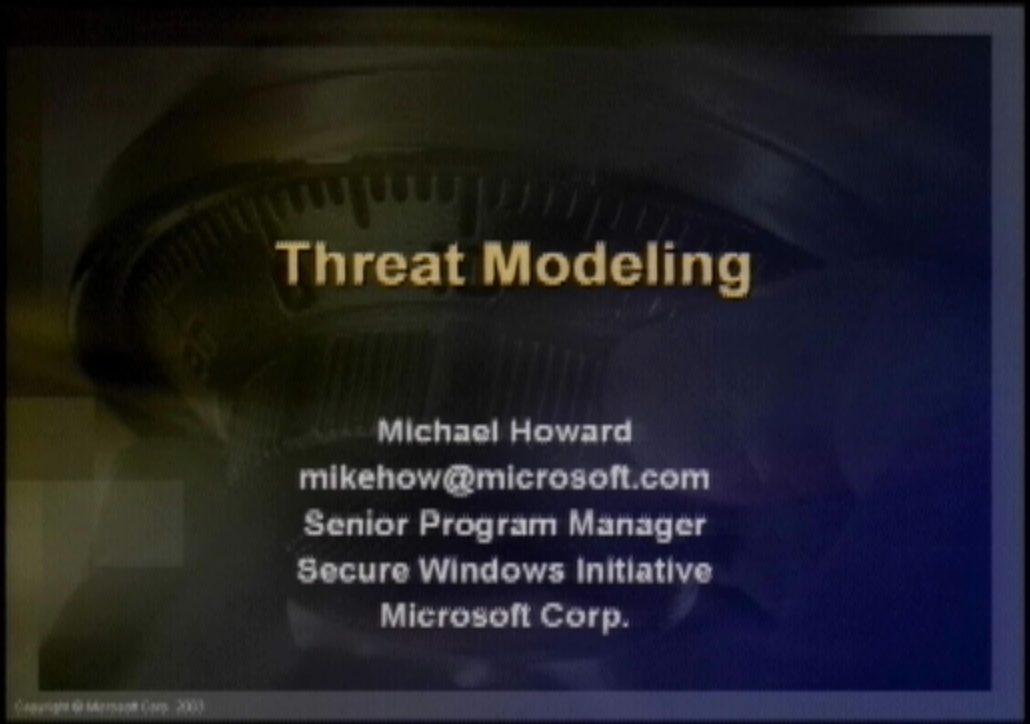

Threat Modeling
Michael Howard
mikehow@microsoft.com
Senior Program Manager
Secure Windows Initiative
Microsoft Corp.
Copyright © Microsoft Corp. 2003

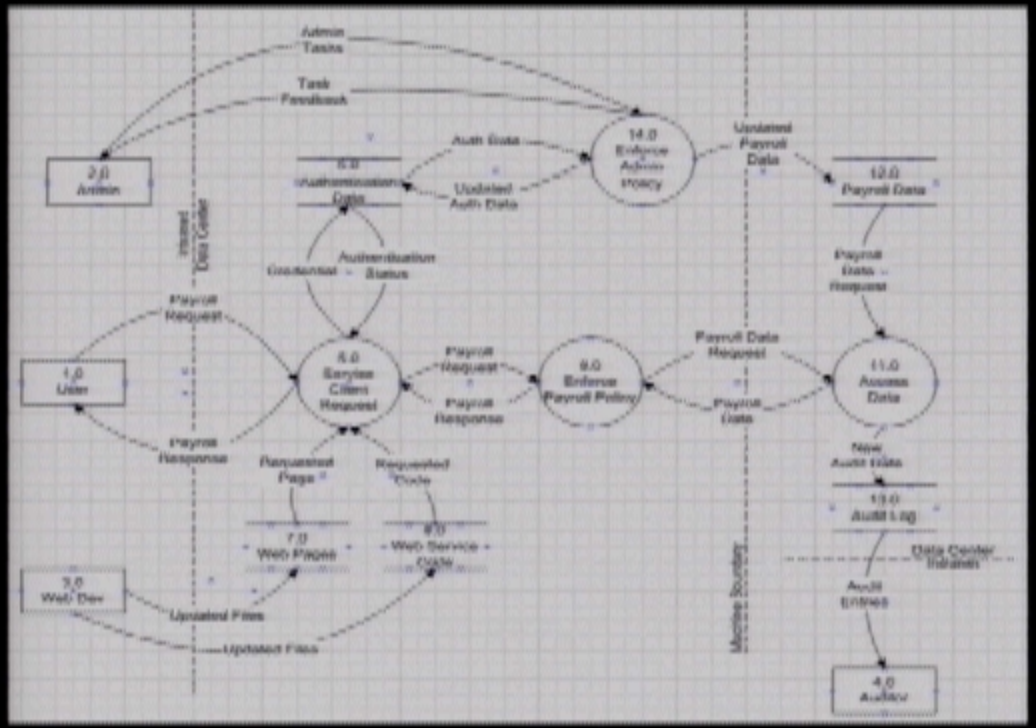

Threat Modeling
Michael Howard
mikehow@microsoft.com
Senior Program Manager
Secure Windows Initiative
Microsoft Corp.
Copyright © Microsoft Corp. 2003

Threat Analysis

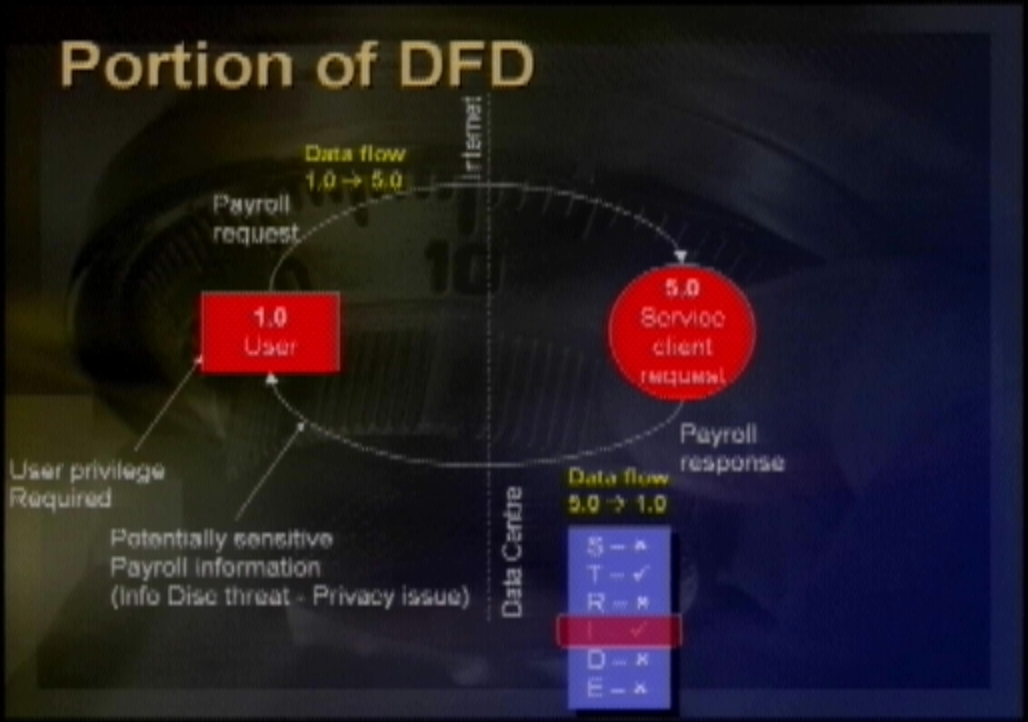
- You cannot build secure applications unless you understand threats
  - Adding security features does not mean you have secure software
  - "We use SSL!"
- Find issues before the code is created
- Find different bugs than code review and testing
  - Implementation bugs vs higher-level design issues
- Approx 50% of issues come from threat models

Threat Modeling Process

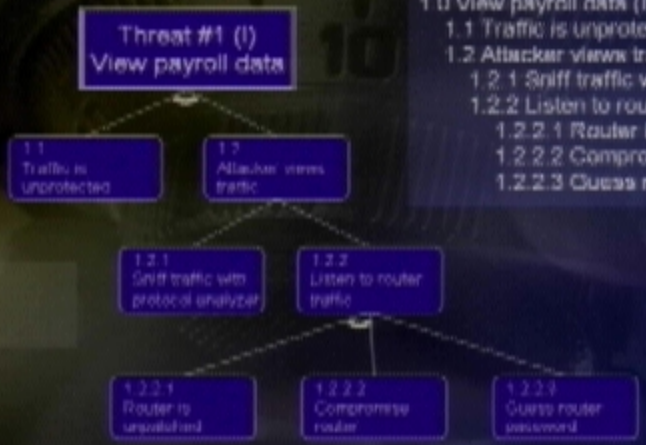
- Create model of app (DFD, UML etc)
  - Build a list of assets that require protection
- Categorize threats to each attack target node with STRIDE
  - Spoofing, Tampering, Repudiation, Info Disclosure, Denial of Service, Elevation of Privilege
- Build threat tree for each threat
  - Derived from hardware fault trees
- Rank threats by risk
  - Risk = Potential * Damage
  - DREAD: Damage potential, Reproducibility, Exploitability, Affected Users, Discoverability


Admin Tasks
Task Feedback
2.0 Admin
Auth Data
14.0 Enforce Admin Policy
Updated Payroll Data
12.0 Payroll Data
Updated Auth Data
Authentication Status
Payroll Data Request
Payroll Request
1.0 User
8.0 Service Client Request
9.0 Enforce Payroll Policy
Payroll Data Request
11.0 Access Data
Payroll Response
Payroll Data
New Audit Data
Requested Page
Requested Code
13.0 Audit Log
7.0 Web Pages
8.0 Web Service Code
Data Center Intranet
Audit Entries
3.0 Web Dev
Updated Files
4.0 Auditor

Portion of DFD

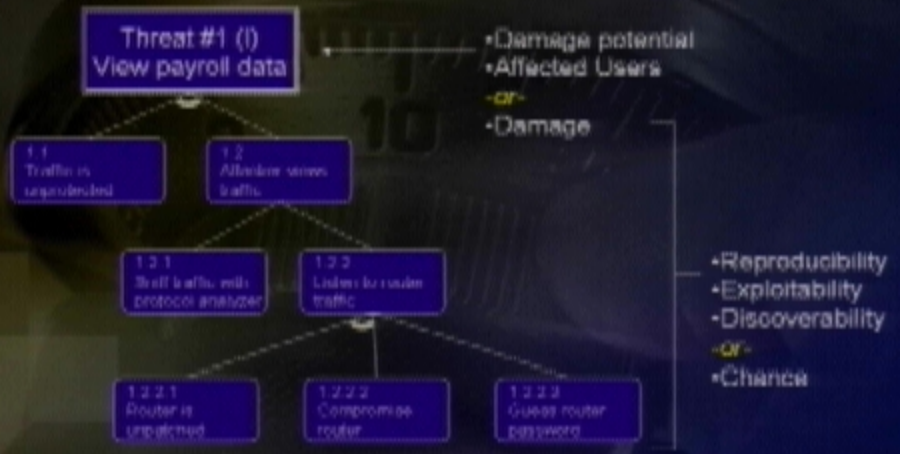


Information Disclosure Threat to Payroll Data



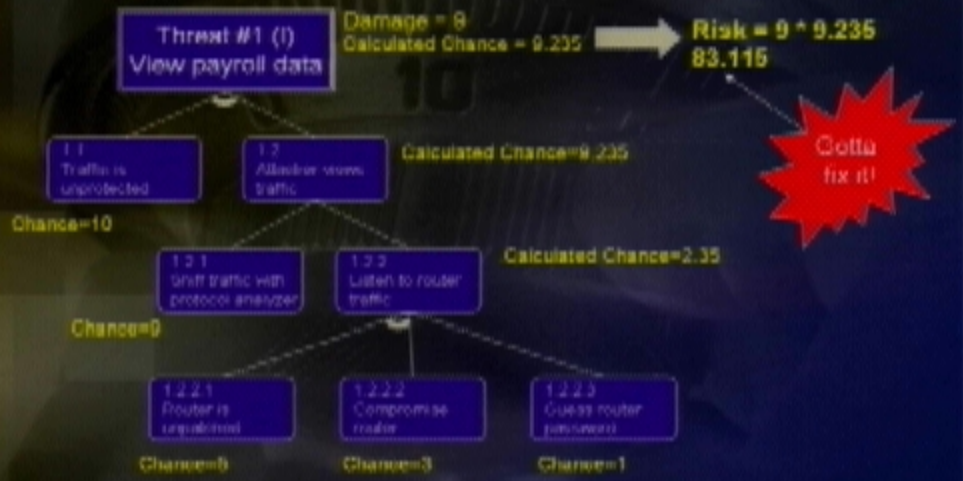
1.0 View payroll data (I)
- 1.1 Traffic is unprotected (AND)
- 1.2 Attacker views traffic
  - 1.2.1 Sniff traffic with protocol analyzer
  - 1.2.2 Listen to router traffic
    - 1.2.2.1 Router is unpatched (AND)
    - 1.2.2.2 Compromise router
    - 1.2.2.3 Guess router password

Applying Risk



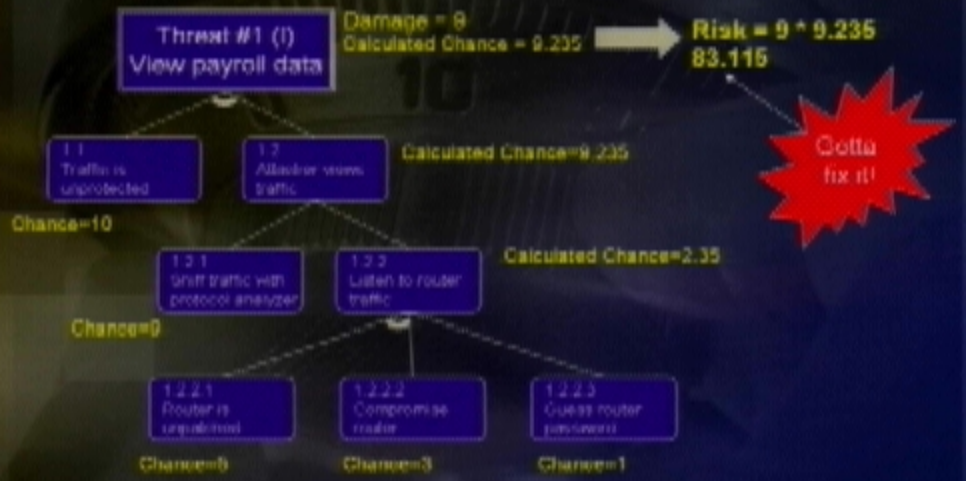
Applying Risk

Using combinatorics and Risk = Chance*Damage



Applying Risk

Using combinatorics and Risk = Chance*Damage

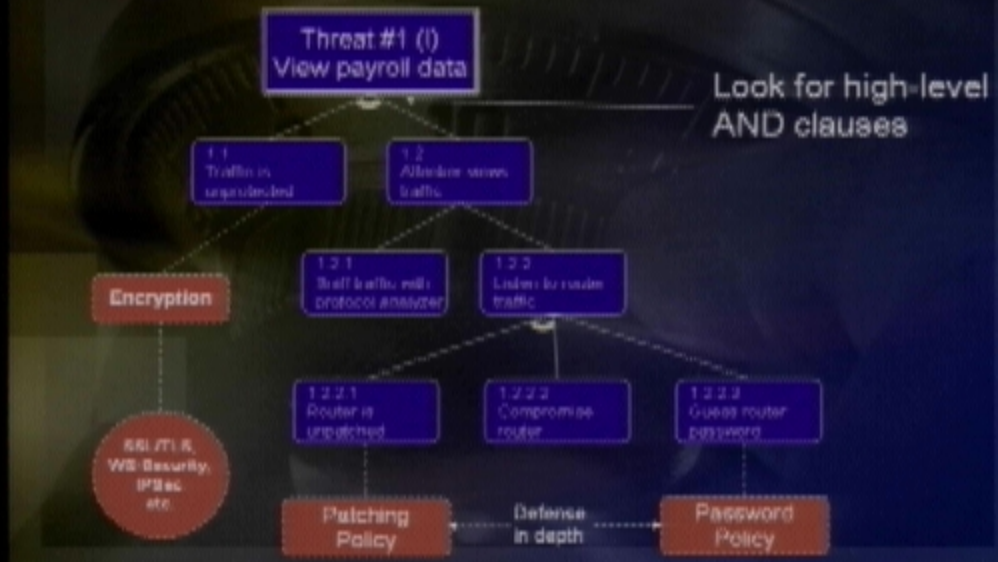


Designing to a Threat Model

- Threat types have mitigation techniques
  - Spoofing
    - Authentication (authn), good credential storage
  - Tampering
    - Authorization (authz), MAC, signing
  - Repudiation
    - Authn, Authz, signing, logging, trusted third party
  - Info Disclosure
    - Authz, encryption
  - Denial of Service
    - Filtering, Authn, Authz
  - Elev of Priv
    - Don't run with elevated privs

Threat Mitigation Techniques & Technologies

Threat Mitigation



Coding to a Threat Model

- Threat models help you determine the most 'dangerous' portions of the application
  - Prioritize security push efforts
  - Prioritize on-going code reviews
  - Help determine the defense mechanisms to use
- Determine data flow
  - "All input is evil, until proven otherwise"

Testing to a Threat Model

- Testers are part of the end-to-end process
- Each threat in the model must have a test plan
- The threat model helps drive testing concepts
- Allows for Whitehat and Blackhat testing
  - Testers should prove the mitigation works
  - Testers should prove they don't work :-)

Testing to a Threat Model

- Mitigation techniques have blackhat testing techniques
  - Spoofing
    - Authentication
      - Brute force creds, cred replay, downgrade to less secure authn, view creds on wire
    - Good credential storage
      - Use Information Disclosure attacks
  - Tampering
    - Authorization
      - Attempt authz bypass
    - MAC, signing
      - Tamper and re-hash?
      - Create invalid hash data
      - Force app to use less secure protocol (no SSL)

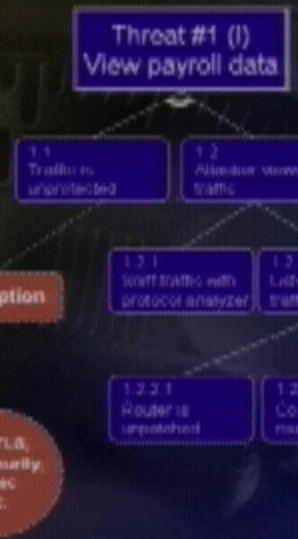
Testing to a Threat Model

- Repudiation
  - Authn & Authz
    - See Spoofing and Tampering
  - Signing
    - See Tampering
  - Logging
    - Prevent auditing, spoof log entries (CR/LF)
  - Trusted third party
    - DoS the third party
- Info Disclosure
  - NOTE: Is there any PII data in the data?
  - Authorization
    - See Tampering
  - Encryption
    - View on-the-wire data
    - Kill process and scavenge for sensitive data
    - Failure leads to disclosure in error messages

Testing Threat Mitigation

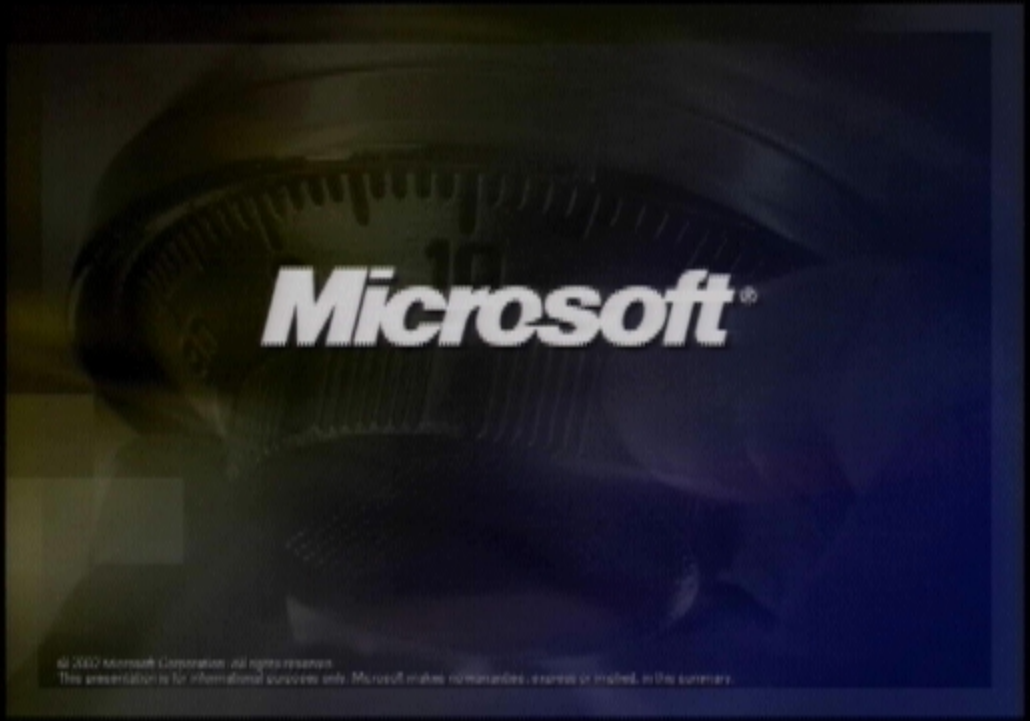
Functionally, is the traffic adequately protected?

Can you force the traffic to be unprotected?
Is the crypto weak?
Where is/are the key(s) stored?
How are the keys exchanged?
Are the defense in depth methods ok?
Are there other conditions?



Threat Modeling Notes

- Scenario-driven
- Determine privilege to initiate data flow
  - Helps determine chance of attack
- Be wary of unauthenticated data flows
- All information disclosure threats are potentially privacy issues
- Any non-mitigated threat is a potential vulnerability
- All security features must mitigate one or more threats
- Work on the higher-risk items first


Microsoft
(c) 2003 Microsoft Corporation. All rights reserved.
This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.